Internet scolaire
&
PROTECTION des MINEURS

Petit guide pratique à l'usage des enseignants et des établissements.

Dossier réalisé par :
Emmanuel LE CLAINCHE
Animateur TICE (DDEC 56) et formateur (IFPB – CNFETP)

Février 2004

Présentation du problème :

A l'heure où l'utilisation d'internet se banalise dans les écoles, collèges et lycées, le problème de la bonne utilisation de l'outil se pose. En effet, si Internet est une mine incontestable de ressources et d'outils, le web constitue en même temps un risque pour les usagers et plus particulièrement pour les mineurs. La présence de sites à caractère pornographiques, violents, racistes, sectaires, etc... aux quels s'ajoutent des sites dont le contenu n'est pas forcément valide doit interpeller l'usager. Ceci pose les enjeux de l'apprentissage de l'utilisation d'internet en milieu scolaire. En effet, le principal enjeu n'est sans doute pas lié à un apprentissage technique, même si le rôle de l'enseignant n'est pas négligeable dans ce domaine, il est davantage d'éduquer le jeune au bon usage de l'outil en le mettant en garde par rapport aux dangers qu'il peut représenter, en développant son esprit critique et en lui donnant des réflexes pour que l'outil soit utilisé de façon raisonnée et responsable.

Les risques :

Ils sont à plusieurs niveaux. Il faut distinguer ici les risques encourus par les élèves et ceux qui sont du ressort de l'éducateur. Certains concernent d'ailleurs aussi bien les élèves que les enseignants.

Sans vouloir en faire un inventaire exhaustif, voici les principaux risques liés à l'usage d'internet encourus pas les élèves et les enseignants :

1. Publication d'information fausse ou inexacte :

   Imaginez un instant qu'un élève de collège aille s'informer sur la seconde guerre mondiale en consultant un site révisionniste. Il est bien évident qu'il n'a pas les connaissances préalables pour s'en rendre compte par lui même et qu'il peut dans ce cas se forger une opinion à partir d'informations fausses et tendancieuses. On comprend donc la nécessité de lui donner quelques clés de lecture et quelques réflexes de recherche de validation de l'information. La première des étapes dans cet apprentissage est sans doute d'amener l'élève à s'interroger sur la validation de l'information et à ne pas prendre l'information comme étant toujours fiable.

2. Contenu de sites pouvant porter atteinte à la dignité humaine :

   Il existe une classification des risques dans ce domaine, l'université de Toulouse tient à jour une liste noire des sites à caractère prohibé, d'autres organismes font également ce travail d'inventaire dans un but de prévention et de protection. Actuellement ceux sont un peu plus de 400 000 sites prohibés qui sont recensés dans ce type de listes. Voici les principales catégories de sites à risques :

Catégories :	***Contenu :***
Adultes	Dans cette catégorie, on peut associer tous les sites à caractères pornographiques. La liste de ces sites est très longue et évolue en permanence. On peut y arriver à partir d recherche tout à fait anodines.
Violence	Dans cette catégorie, on peut classer tous les sites incitant à la haine, la perversion et à la violence.

Catégories :	*Contenu :*
Drogue	Ici, on retrouve aussi bien les sites qui se donnent comme objectif de banaliser l'idée que la drogue n'est pas dangereuse, qu'elle peut même « être bonne » pour l'individu, que les sites d'incitation à l'usage de produits en passant par les sites de réseaux organisés qui utilisent internet pour fournir leur marchandise, etc.
Piratage	On retrouve ici les sites d'incitation à pirater, les sites qui proposent des produits piratés (logiciels, musiques, films, photos, oeuvres en tout genre...). On pourrait aussi y ajouter les sites, qui par les procédés qu'ils mettent en oeuvres (Peer to peer), n'offrent pas la garantie que les produits proposés en télé chargement le sont dans un cadre légal.
Publicité	Dans cette catégorie on retrouve les innombrables sites qui proposent de la publicité non désirée (pop up, spam...), certains messages pouvant d'ailleurs avoir un contenu plus que douteux.
Sectes	Les sites de cette catégorie sont des sites présentant l'activité ou la philosophie de sectes mais ils peuvent aussi être des sites à la présentation anodine qui par le biais de procédés sournois peuvent avoir pour objectifs d'influencer, de manipuler, de recruter ou de récupérer des informations à caractère privé...
Racisme	Ces sites font l'éloge du racisme ou en banalisent les effets. Ils peuvent inciter à la violence et à la haine ou avoir un objectif plus sournois d'influencer le visiteur dans le but de banaliser les idées afin de manipuler, voire de recruter des adeptes.
Échanges, rencontres	Cette catégorie est souvent très prisée des jeunes, ils éprouvent du plaisir à échanger sur le web, en particulier avec des gens qu'ils ne connaissent pas. Ils faut savoir cependant que ce type d'échanges sur internet fait prendre des risques : ➢ Le jeune peut avoir tendance à se défouler, se libérer. Comme il pense qu'il n'est pas connu, il estime qu'il peut tout se permettre... ou presque... Cela donne une idée de la teneur de certains dialogues sur le « chat ». ➢ Il est fréquent que le jeune mente sur son âge, il se fait passer pour un adulte lorsqu'il échange sur un site où les membres sont plus âgés que lui, de même, lorsqu'il est sur un site réservé à des adolescents rien ne prouve qu'on n'y trouve que des adolescents. ➢ Ces réseau d'échanges sont la plupart du temps incontrôlables, certains de ses membres sont pour le moins peu fréquentables, rien ne garantit que les personnes qui participent aux échanges n'ont pas des intentions déplacées ou perverses. ➢ Le jeune qui n'a pas été informé des dangers ou qui aurait une curiosité éveillée aura une attitude à risque, il pourra dans certaines circonstances céder à la tentation de s'inscrire sur le site, de laisser ses coordonnées, son adresse e-mail pour pouvoir être contacté personnellement, etc... ➢ Dans cette catégorie de sites, nous allons retrouver les sites d'échanges un peu particulier : échangistes, rencontres « érotiques », donc contre indiqués pour des jeunes mineurs, etc.

Catégories :	*Contenu :*
Tricherie	Et oui, cela existe, au lieu de se farcir l'exercice ou la traduction d'un texte, il est plus aisé de le faire faire sur internet, c'est plus amusant, bien moins fatigant... mais peut-être moins efficace.

3. Atteinte à la vie privée :

Dans cette catégorie, on peut citer les sites qui par le biais d'artifices plus ou moins voyants récupèrent des informations à caractère privé sur les visiteurs. Si la navigation sur internet peut donner un sentiment de grande liberté pour l'internaute, il faut savoir aussi que c'est un lieu d'atteinte manifeste de la vie privée, donc d'atteinte à la liberté des personnes.
Cette atteinte à la vie privée peut se faire de différentes manières, cela va de la demande abusive de formulaires à compléter; d'inscriptions à effectuer en ligne, à des méthodes plus sournoises d'enregistrement de cookies, chevaux de troie ou d'espiogiciels (logiciels espions) sur les disques durs des usagers.

4. Endommagement du poste informatique de l'usager :

C'est le résultat des virus qui ont trouvé avec internet un vecteur de communication et de dispersion très efficace. Les effets de ces derniers sont plus ou moins importants. S'ils encombrent les réseaux de communication, il faut savoir qu'ils peuvent aussi sérieusement endommager les ordinateurs et provoquer des pertes de données importantes, voir des transmissions de données personnelles à caractère privé vers l'extérieur à l'insu de l'utilisateur.

5. Piratage ou complicité dans des actes de piratage :

On a ici deux niveaux de risques lié au fait que l'acte de piratage peut être conscient ou inconscient, il n'empêche que dans les deux cas il est prohibé. Certains sites se présentent ouvertement comme des sites incitant à pirater ou proposant des outils et des méthodes pour pouvoir pirater. Il est évident que cela est totalement illégal et qu'aucune raison ne peut justifier cet acte. Sur d'autres sites, le risque est d'une autre nature dans la mesure où le visiteur peut, sans le savoir, télécharger un produit illégal. C'est assez fréquent pour les logiciels dont certains sont annoncés comme étant gratuits et libres de droits sur certains sites alors qu'un passage sur le site de l'auteur enlève toute ambiguïté en affichant les tarifs du produit. C'est aussi le cas dans d'autres domaines tels que celui de la musique ou du film en particulier.

A cela s'ajoute des risques supplémentaires pour l'éducateur ou l'élève majeur :

1. Responsabilité juridique :

Dans le cadre scolaire, la responsabilité de l'enseignant et de l'établissement est engagée quand des actes illicites sont commis. Ce qui est vrai dans les domaines les plus courants s'applique aussi à l'usage d'internet. Cela suppose par conséquent que l'établissement prenne ses responsabilités dans ce domaine et cela suppose aussi que l'enseignant mesure bien son niveau de responsabilité et qu'il adopte une attitude en conséquence.

Ce que dit la loi :

Au sujet de la protection des mineurs, la lecture des textes de lois est un préalable incontournable. Il est possible de consulter les textes en vigueur à l'adresse : https://www.internet-mineurs.gouv.fr/frameset/framset_textescodepenal.html

D'autres sites sont à découvrir dans ce domaine, en voici quelques uns :

- Consulter le guide juridique de l'internet scolaire à l'adresse : http://www.educnet.education.fr/juri/juriscol/fiche06.htm
- Consulter le compte rendu d'une conférence portant sur « L'approche juridique dans l'accès à des ressources en ligne » . Cette conférence organisée sous l'égide du Rectorat de Lyon s'adressait à des documentalistes.

Adresse de la ressource :
http://www2.ac-lyon.fr/enseigne/documentation/internet/gerer/droit/rousset.html

Des ressources sur le sujet :

Il y en plusieurs, elles se recoupent souvent, elles sont la plupart du temps proches des ressources proposées dans le cadre de la protection parentale dans la mesure où le problème est sensiblement identique dans les deux cas.

Voici quelques adresses incontournables :

- Consulter le dossier réalisé sur ce sujet par le Café pédagogique : http://www.cafepedagogique.net/dossiers/securite/danger.php
- Quelques conseils juridiques de bon sens proposés par l'académie de Besançon : http://artic.ac-besancon.fr/juridique/conseils.htm
- L'Europe travaille aussi sur le sujet et propose un programme spécifique appelé Educaunet, ce programme est complété par une proposition de solution (ICRA). Pour s'informer sur le programme Ecucaunet : http://www.educaunet.org/article.php3?id_article=31
- A consulter également un dossier très complet réalisé par l'UNAF. Ce dossier est consultable à l'adresse : http://www.unaf.fr/article.php3?id_article=129%20
- La délégation « Internet » du gouvernement propose également un tour d'horizon du problème à l'adresse : http://accespublic.internet.gouv.fr/actions/protection.htm
- Consulter le dossier de la revue « 60 millions de consommateurs » : http://www.60millions-mag.com/page/bases.11_actualites./

Des outils de filtrage pour se protéger :

Il en existe un certain nombre, pas tous aussi efficaces, certains sont payants, d'autres gratuits, certains sont assez simples à mettre en oeuvre, d'autres réservés à des spécialistes avertis. Certains proposent une solution globale au niveau des réseaux, d'autres sont des solutions de protection mono postes. Beaucoup des solutions existantes sont hélas en anglais, ce qui ne facilite pas leur mise en oeuvre. Une certitude cependant, si ces outils sont des garde fous sécurisant, ils ne suffisent cependant pas en raison de leur quasi impuissance à éduquer et c'est dans ce domaine que le rôle et l'attitude de l'enseignant sont essentiels. On ne peut pas se dérober et se dé responsabiliser sous prétexte que l'établissement est en sécurité derrière de bons filtrages et des possibilités de suivi

et de contrôle, on a le devoir d'éduquer au bon usage de l'outil.

Quelques outils de filtrage parmi d'autres :

a) le solutions légères :

Outils	*Téléchargement*	*Réseau*	*Mono poste*	*Commentaires*	*Les +*	*Les -*
IP Free (iProtectYou)	http://www.downlinx.com/proghtml/4/404.htm ou à : http://www.tucows.com/preview/295406.html		x	➢ C'est une solution intéressante si elle est est bien paramétrée. ➢ Elle est particulièrement bien adaptée pour du filtrage parental.	➢ Elle est simple à mettre en oeuvre. ➢ Elle est protégée par mot de passe. ➢ Elle permet d'assurer un contrôle à posteriori des connexions, voire des activités sur le poste. ➢ Elle est très efficace lorsque le paramétrage est bien fait (1). ➢ C'est une solution très complète qui ne se résume pas au blocage de sites web.	➢ Elle est en anglais (mais je peux fournir un mode d'emploi en français sur demande). ➢ Il faut parfois la désactiver avec les logiciels de messagerie (filtrage de pub). ➢ Elle est longue à paramétrer (impossibilité d'importer des listes de mots ou d'adresses prohibés).
Proxomitron	http://www.proxomitronfr.fr.st/	(Peut-être mais pas encore testé)	x	➢ C'est une solution gratuite qui a été traduite en français. ➢ C'est un mini proxy. ➢ Elle est simple à mettre en oeuvre si on suit le mode d'emploi proposé à l'adresse ci-contre. ➢ Elle s'adapte aussi bien à la protection en milieu scolaire qu'en protection parentale.	➢ Elle est facile à mettre en oeuvre. ➢ Elle est gratuite et traduite en français. ➢ Son filtrage est efficace quand le paramétrage est complet et bien fait. (1) ➢ Elle permet l'utilisation de « blocklists » avec possibilité de récupération de listes noires.	➢ Elle ne permet pas un contrôle à posteriori (traçabilité). ➢ Elle est facile à désactiver par l'élève.

Outils	*Téléchargement*	*Réseau*	*Mono poste*	*Commentaires*	*Les +*	*Les -*
Muffin	http://muffin.doit.org/ ou http://nicolasfr.free.fr/fr/index.html		x	➢ C'est une solution développée en langage Java, ceci suppose par conséquent des compétences pour sa mise en oeuvre. ➢ Elle est reconnue par l'Éducation Nationale.	➢ Elle est gratuite. ➢ Elle est (d'après ce que l'on peut en lire) efficace.	➢ Sa mise en oeuvre suppose des compétences particulières (environnement java).
SurfPas	http://www.cogilab.com/fr/homeedition/		x	➢ Il est gratuit pour un usage familial mais payant pour un usage en établissement scolaire.	Je ne l'ai pas testé.	
ICRA Plus	http://www.icra.org/_fr/icraplus/			➢ C'est la solution proposée par le programme européen Educaunet. ➢ C'est une solution gratuite, mais qui propose des compléments payants. ➢ Son principe repose sur un accès limité à la liste des sites que le programme ICRA a validé. ➢ Tout utilisateur peut demander la validation de sites à l'ICRA pour que ceux soient accessibles.	Je l'ai peu testé.	
Utiliser un vrai proxy.	Voir les compléments d'information en b) ci-dessous.	x		➢ C'est la solution idéale.	➢ C'est une solution complète et efficace. ➢ L'élève n'a pas la possibilité de la désactiver. ➢ Elle permet de centraliser le système de protection.	➢ Elle suppose des compétences pour sa mise en place. ➢ Elle nécessite qu'on dédie un poste à cet effet (serveur web). ➢ Les solutions gratuites existantes nécessite une connaissance de Linux.

b) Les solutions plus professionnelles mais aussi plus lourdes à mettre en oeuvre :

Elles font appel à la mise en oeuvre d'un proxy. Il existe plusieurs solutions dans ce domaine. Voici quelques adresses qui permettent de se faire une idée d'une partie des solutions qui existent :
http://www.ac-creteil.fr/reseaux/internet/inet/proxy/default.htm

http://www.ac-creteil.fr/reseaux/internet/inet/proxy/client-proxy.htm

Quelques solutions Proxy : SquidGard, Wingate, Apache, Sambar...

(1) Toute solution, aussi bonne soit-elle peut s'avérer d'une efficacité variable résultant de la qualité de l'intervention humaine, en particulier lors de la configuration. L'importance de la mise à jour des données de filtrage est un élément essentiel. Les solutions légères proposées dans ce document ne permettent pas d'automatiser les tâches de mise à jour. Il faut donc partir du fait que le risque zéro n'existe pas et que la machine n'est pas infaillible. Par conséquent, si un système protégé limite les risques d'incident, on ne peut pas admettre qu'il les élimine totalement, l'attitude et la vigilance de l'enseignant ne doit donc pas se relâcher dans ce domaine.

L'éducation est un enjeu capital : l'élaboration d'une charte d'utilisation d'internet en milieu scolaire.

En effet, si on se limite à mettre des sécurités en place pour éviter que les élèves puissent aller sur des sites prohibés, on passe à côté du travail essentiel que nous avons à réaliser dans ce domaine. Ce n'est pas parce que l'accès à internet est sécurisé au collège ou au lycée que internet devient sécurisé. L'élaboration d'une charte d'utilisation de l'outil multimédia impliquant les enseignants et les élèves est une porte d'entrée intéressante pour aborder l'aspect éducatif. C'est la charte qui donne du sens aux stratégies de sécurité mises en place dans l'établissement, l'élaboration de celle-ci devrait constituer une temps de formation et d'éducation important, elle doit concourir à faire découvrir les risques et à développer des réflexes et des attitudes pour que le jeune soit informé et devienne un internaute responsable même quand il n'est plus à l'intérieur de son établissement scolaire.

Voici quelques adresses proposant des pistes pour l'élaboration des chartes d'utilisation d'internet :

- Un projet de charte est télé chargeable sur le site d'Edcunet.
  http://www.educnet.education.fr/
- Une ressource proposée par l'académie de Besançon :
  http://artic.ac-besancon.fr/juridique/charte_tice.htm
- Un document (pas très digeste) proposé par l'académie de Lyon. Si celui-ci est autère, il n'en demeure pas moins complet.
  http://www2.ac-lyon.fr/etab/lycees/lyc-69/jpsartre/site_lycee/fichiers/charte/charte2p.html
- Utilisation d'internet au CDI : Une ressource proposée par l'académie de Dijon :
  http://webpublic.ac-dijon.fr/pedago/cdi/charte.htm

Autres adresses incontournables :

Informatique et Liberté : le site de la CNIL : http://www.cnil.fr/
Lutter contre le spam avec CASPAM : http://www.caspam.org
Virus, chevaux de troie, spywares, canulars... et compagnie : http://www.secuser.com ou http://www.hoaxbuster.com/

En guise de conclusion :

Ce dossier est un document provisoire qui devrait se compléter progressivement. Vos observations seront les bienvenues pour l'améliorer, n'hésitez pas à les transmettre. Vous pouvez le

diffuser dans vos établissements sous réserve d'en mentionner la source, tel qu'il est il devrait déjà permettre de répondre à de nombreuses questions souvent soulevées sur le sujet.

Emmanuel LE CLAINCHE
Animateur TICE (DDEC 56)